VIRUSTOTAL

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Display grouped sandbox reports

Zenbox Linux	0	5	0	0	2	0

Activity Summary

Download Artifacts Full Reports Help

Detections

NOT FOUND

Mitre Signatures

6 INFO

IDS Rules

NOT FOUND

Sigma Rules

NOT FOUND

Dropped Files

1 GZIP

Network comms

NOT FOUND

Behavior Tags

detect-debug-environment sets-process-name

MITRE ATT&CK Tactics and Techniques

Search for technique, subtechnique and in its matching entries

None Info

Execution
TA0002 1 Techniques

Scripting
T1064

1

Persistence
TA0003 2 Techniques

Create or Modify S
T1543

Behavior Similarity Hashes

Zenbox Linux… 532dd8d49eff2a3d52b4084223ac6797

File system actions

Files Opened

/dev/urandom
/etc/dconf/profile/user
/etc/fonts/conf.avail
/etc/fonts/conf.avail/10-antialias.conf
/etc/fonts/conf.avail/10-autohint.conf
/etc/fonts/conf.avail/10-hinting-full.conf
/etc/fonts/conf.avail/10-hinting-medium.conf
/etc/fonts/conf.avail/10-hinting-none.conf
/etc/fonts/conf.avail/10-hinting-slight.conf
/etc/fonts/conf.avail/10-no-sub-pixel.conf

Files Written

/root/.cache/dconf/user

/var/log/auth.log.1.gz

/var/log/kern.log.1.gz

Files Dropped

/var/log/auth.log.1.gz

/var/log/kern.log.1.gz

Process and service actions

Processes Created

- /bin/gzip
- /bin/sh sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/mail.info/var/log/mail.warn/var/log/mail.err/var/log/mail.log/var/lo
- /bin/sh sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
- /usr/bin/dbus-launch dbus-launch --autolaunch=a39eb3ed78b7401fb6809ed0c562a5b1 --binary-syntax --close-stderr
- /usr/bin/engrampa engrampa /tmp/SwissIO_Fixed.zip
- /usr/bin/exo-open -
- /usr/bin/exo-open exo-open /tmp/SwissIO_Fixed.zip
- /usr/bin/systemctl systemctl kill -s HUP rsyslog.service
- /usr/lib/p7zip/7z l -slt -bd -y -- /tmp/SwissIO_Fixed.zip
- /usr/lib/rsyslog/rsyslog-rotate

Shell Commands

- /bin/gzip
- /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh engrampa /tmp/SwissIO_Fixed.zip
- /usr/lib/p7zip/7z l -slt -bd -y -- /tmp/SwissIO_Fixed.zip
- /usr/lib/rsyslog/rsyslog-rotate
- 7z l -slt -bd -y -- /tmp/SwissIO_Fixed.zip
- dbus-launch --autolaunch=a39eb3ed78b7401fb6809ed0c562a5b1 --binary-syntax --close-stderr
- engrampa /tmp/SwissIO_Fixed.zip
- sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/mail.info/var/log/mail.warn/var/log/mail.err/var/log/mail.log/var/lo
- sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog
- systemctl kill -s HUP rsyslog.service

Processes Tree

- 4989 - /usr/bin/exo-open exo-open /tmp/SwissIO_Fixed.zip
  - 4991 - /usr/bin/dbus-launch dbus-launch --autolaunch=a39eb3ed78b7401fb6809ed0c562a5b1 --binary-syntax --close-stderr
  - 4993 - /usr/bin/exo-open -
- 4994 - /usr/bin/engrampa engrampa /tmp/SwissIO_Fixed.zip
  - 4997 - /usr/bin/dbus-launch dbus-launch --autolaunch=a39eb3ed78b7401fb6809ed0c562a5b1 --binary-syntax --

close-stderr

5005 - /usr/lib/p7zip/7z l -slt -bd -y -- /tmp/SwissIO_Fixed.zip

4942 - /bin/sh sh -c /usr/lib/rsyslog/rsyslog-rotate logrotate_script /var/log/syslog

4943 - /usr/lib/rsyslog/rsyslog-rotate

4944 - /usr/bin/systemctl systemctl kill -s HUP rsyslog.service

4945 - /bin/gzip

Highlighted actions

Highlighted Text

""